# PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 1/00, 12/14	**A1**	(11) International Publication Number: **WO 00/70427**
		(43) International Publication Date: 23 November 2000 (23.11.00)

(21) International Application Number: PCT/FI00/00448

(22) International Filing Date: 18 May 2000 (18.05.00)

(30) Priority Data:
991134   18 May 1999 (18.05.99)   FI

(71) Applicant *(for all designated States except US)*: SONERA SMARTTRUST OY [FI/FI]; c/o Sonera Oyj, P.O.Box 106, FIN–00051 Sonera (FI).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: HILTUNEN, Matti [FI/FI]; Otakuja 2 B 27, FIN–02150 Espoo (FI). MIETTINEN, Jarmo [FI/FI]; Everstinkatu 1 C 72, FIN–02600 Espoo (FI). NORDBERG, Marko [FI/FI]; Itämerenkatu 12 D 74, FIN–00180 Helsinki (FI). LIUKKONEN, Jukka [FI/FI]; Kaarlenkatu 10 B 59, FIN–00530 Helsinki (FI).

(74) Agent: PAPULA OY; P.O. Box 981 (Fredrikinkatu 61 A), FIN–00101 Helsinki (FI).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
In English translation (filed in Finnish).

(54) Title: METHOD AND DEVICE FOR AUTHENTICATING A PROGRAM CODE
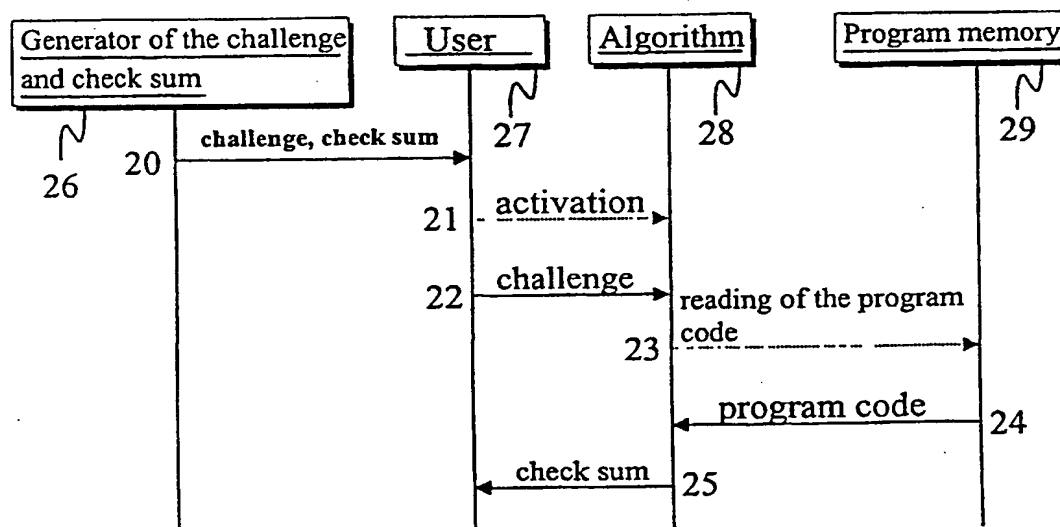
(57) Abstract

The invention relates to a method and system for authenticating a program code. In the method, a first check sum is computed at the program code, the computed check sum is compared with a second check sum known to be valid and in response to the aforementioned comparison the program code is proved to be authentic in case the first check sum matches with the second check sum. Further, a predetermined challenge is added to the program code after which the aforementioned first check sum is computed at the combination of the program code and the challenge. In this way, the applications used in applications demanding high security may be certified dependably and variably. In that case, the users of software may count on the authenticity of the data processed, e.g. on the display of a mobile phone or a keyboard throughout the whole process.

SDOCID: <WO___0070427A1_I_>

1

Method and device for authenticating a program code.

SCOPE OF THE TECHNIQUE

5   The invention relates to communication sys-
tems. One specific objective of the invention is a
method and system for testing the reliability of soft-
ware.

The objective of the invention is a method
for authenticating a program or program code stored on
10   a storage device in which method a first check sum is
computed at the program code, the check sum is com-
pared with a second check sum known as valid and in
response to the aforementioned comparison the program
code is proved to be authentic in case the first check
15   sum matches with the second check sum.

BACKGROUND OF THE INVENTION

Mobile networks, i.e. GSM networks (GSM,
Global System for Mobile communications) have recently
20   become very popular. The additional services connected
with the mobile networks have correspondingly in-
creased at an accelerated tempo. The application
fields are most versatile. The mobile telephone may be
used as a means of payment for, e.g. petty purchases,
25   such as soft drinks and car wash automates. Everyday
activities, such as payment transactions, bank serv-
ices etc, have been added, and will be added also in
the future, to the functionality of present mobile
phones. The mobile stations of the next generation
30   will be more advanced in respect of the service level
and data transfer capacity compared with the previous
ones.

With the aid of digital signing, which is re-
garded as a general requirement in electronic payment,
35   it is possible to make sure of the coherency of the
information to be sent and identify the source ad-

dress. The digital signature is derived by encrypting
the check sum computed at the information to be sent
with a sender's private key. As nobody, except the
sender, knows the private key, the recipient may, when
5   decoding the encryption with the sender's public key,
make sure that the information is unmodified and gen-
erated by using the private key only known to the
sender. An example of an algorithm used in digital
signing is a RSA ciphering algorithm, which is an en-
10 cryption system of both the public key and the private
key and which is also used for encrypting messages.

In the public key infrastructure the user
keeps the private key only to himself/herself, but the
public key is available to all entities. It is not
15 enough that the public key is stored as such, e.g. in
an electronic mail directory, because somebody might
forge it and appear as an authentic holder of the key.
Instead, certification and certificates are needed,
which serve as a proof given by the trusted party
20 (certification authority) of the fact that the name,
identification number and public key belong to the
same person. The certificate is usually a combination
consisting of a public key, name and identification
number etc, which the certification authority signs
25 with his/her private key.

When the recipient of a digitally signed mes-
sage wishes to make sure of the authenticity of the
message, at first he/she has to obtain the digital
certificate, which gives him/her the public key and
30 the name. After that he/she has to authenticate the
certificate. To be able to perform this he/she may
have to obtain some more additional certificates (a
cerfication chain), which have been used to authenti-
cate the certificate in question.

35 In case the certificate is authentic, the re-
cipient authenticates the message by using the public
key received along with the certificate. If the signa-

ture passes the test, the sender is the person identified by the certificate. In certification, a special block list is used in which the certificates taken out of use are entered. Directory services are needed for
5 both the certificates and the block list.

Mobile phones have been implemented by using at least partly embedded systems and software. In this case, the modifying of the original software and functions is possible, at least partly. With a modified
10 software the content of electronic payment messages may be changed with intent to defraud by changing the account numbers, sums liable to payment, digital signatures etc, and at the same provide the user with the correct information about the transactions.

15 At the present time it is impossible for the user to check, if the mobile phone he is using is provided with the original software made by the manufacturer or some kind of modified version. In case the mobile phone is used for bank services, as a means of
20 payment etc, the user has to be able to check that the device is provided with the valid, original software version.

The most important thing for the user is to be able to check the reliability of the display and
25 key board, the security, the originality of the parts associated with the security, such as storage of the subscriber identification data, the pass words and key codes as well as the security and reliability of the communication channels used by the device. In addi-
30 tion, the user has to be able to check the software randomly, at an unpredictable moment so that the software is not beforehand prepared to be checked.

In principle, a software may be checked by using a so called direct checking in which case two
35 independent check sums, effective enough, are computed on the mobile phone software, e.g. using a hash function SHA-1, MD5 or an equivalent and effective Hash

4

function. The first check sum is computed on the mo-
bile phone and the second check sum is computed by the
supplier of the original software. The first and the
second check sum are compared with each other and in
5   case they match, the software of the telephone is
original. However, the problem associated with this
solution is the fact that a modified or forged soft-
ware may ignore the programmatic computation coded in
the program and print only the original check sum as
10   if it were the first check sum, when so requested by
the user.

THE OBJECTIVE OF THE INVENTION

      The objective of the invention is to elimi-
15   nate or at least reduce the drawbacks referred to
above. One specific objective of the present invention
is to disclose a method and system for reliable check-
ing of the authenticity and validity of software in a
mobile station, though the invention may be used for
20   testing of any kinds of software.
      A further objective of the invention is to
disclose a reliable and variable method by using which
different service providers and users of the services
may make sure of the authenticity of the devices and
25   programs used by them.
      As for the features characteristic of the in-
vention, reference to them is made in the claims.

SUMMARY OF THE INVENTION

30   The main principle of the method of the in-
vention is to use for checking so called direct check-
ing. In this procedure the manufacturer of the origi-
nal software announces a variable challenge or set of
challenges and a response or check sum corresponding
35   to each of the challenges. The challenge is chosen
from a group, which consists of a character string,

program function and input. When the user at a random moment wishes to check the authenticity of the software he/she is using, he/she stores or inputs the challenge into the device, e.g. mobile phone, which is
5 using the software. The challenge is stored in the same memory as the software after which the device computes the check sum, i.e. the response, at the memory space by using a check algorithm. The device gives this response to the user, who compares it with the
10 response corresponding to the given challenge and in case the responses match, the user knows that the software is authentic and original. By using this kind of procedure, it is possible to compare with each other two programs with the same origin. When using a
15 software known as secure and randomly chosen challenges, the responses given by a safe software may be compared with the responses given by the software to be checked.

The user may retrieve the challenge and the
20 check sum corresponding to it, e.g. from the database, which is maintained on a safe network server available to the user, or in any type of media the user has access to. In the same database may also be maintained the valid program codes into which the user may input
25 the same challenge as into his/own device and thereby compare the check sum given by his/her own device with the one given by the valid program code.

In the method of the invention, a first check sum is computed at the program code, the check sum is
30 compared with a second check sum known as valid and in response to the aforementioned comparison the program code is proved to be authentic, in case the first check sum matches with the second check sum.

According to the invention, a challenge is
35 added to the program code, and only after this the aforementioned first check sum is computed at the combination of the program code and the challenge. In

this application, the challenge is an input, a certain character string or corresponding data added to the program code by using which the computation is bound to a give certain outcome. In one application of the invention, the program code and the challenge are stored in the memory space and the check sum is computed at the whole memory space, wherein the aforementioned program code and challenge are stored. The challenge to be added may be modified by using an appropriate algorithm, which produces a challenge of standard format to be added to the program code no matter how the character string is. In this case, the addition of the challenge in the program code may be standardised, which makes the authentication easier to be implemented. For example the algorithm SHA-1 always produces a 160 bit long challenge regardless of the challenge length, which challenge as being of standard length may be added to the program code. However, the hashing of the original challenge before adding it to the program code does not effect the reliability or function of the challenge and check sum pair, provided that the challenge is hashed by using an algorithm known to everyone, which always produces the same hash from the original challenge.

A memory area, the size of a challenge, in the software or program code to be checked, may be substituted with a challenge; the challenge may be added to the memory area or alternatively, the memory area may be left blank in which case the challenge is in fact an empty character string. In addition, adding the challenge may mean removing a certain program code part before computing the check sum. In all of these cases, the check sum computed at the memory space is unique and unpredictable and depending solely on the combination of the program code and the challenge.

In one application of the present invention, the challenge and the check sum corresponding to it

are chosen from a group of random challenges, which comprises of challenges and check sums corresponding to them. New pairs of challenge and check sum may be constantly generated, which makes the deceiving even

5   more difficult. Moreover, by choosing the challenges and the check sums corresponding to them in such a way that the freed memory cannot be used for storing the check list, the reliability is improved at the same. Moreover, it is important that the storage device is

10   not connected to the external database, terminal device or any other device, where it could retrieve or request the check sum corresponding to the challenge. It is important that the necessary computing routines are carried out solely by the local software.

15   In another application of the invention, an authenticated program code may be used for the authentication of other program codes included in the same software or system in such a way that the check sum of the authenticated program code is compared with the

20   one given by other program codes over the same challenge. This concerns, e.g. the use of an authenticated program code of a first user for the authentication of the program code of a second user. In one application, the mobile phone of the first user might transmit a

25   message to the mobile phone of the second user. The message would inform the challenge, which the user of the second mobile station could use for testing of his/her software. The same solution may be used for automatic testing in such a way that network transmits,

30   e.g. during the initialisation of the call, a challenge to the telephone to which the telephone responds by transmitting the computed check sum. If the check sum is not valid, the network makes the necessary conclusions and informs the user as well as other necessary

35   parties about the matter.
           An advantage of the invention compared with the prior art is the fact that due to the invention

8

embedded systems or software known as reliable may be
implemented the reliability of which may be checked
after certain periods of time.

A further advantage of the invention in com-
5   parison with the prior art is the fact that the com-
puting of the check sum does not need to be an exter-
nal function, instead it may be integrated in the
software to be checked. Moreover, the solution of the
invention makes it unnecessary to use the method of
10   both the public key and the private key.

Moreover, random access memory is needed
less, because the program code does not need to be de-
coded or modified in the device. Moreover, due to the
dynamics of the challenge and the check sum corre-
15   sponding to it, the check sum corresponding to the
challenge may not be known beforehand. In this case,
the generation of the challenges may be done com-
pletely randomly.

20   **DRAWINGS**

In the following section, the invention is
described by referring to the attached drawings in
which

Fig. 1 schematically represents a device of
25   the invention.

Fig. 2 represents the function as described
in the invention by using a block diagram and

Fig. 3 represents one example of computing
the check sum as described in the invention.
30

DESCRIPTION OF THE INVENTION IN DETAIL

The device of fig. 1 comprises of memory 1,
processor 2, receiving block 3, display 4 and input
device 5. The memory is divided into a static part A
35   and dynamic part B. The size of the dynamic part B is
chosen in such a way that the check sum corresponding

to the challenge does not fit to be stored in it, in
order to reduce deceiving. Memory 1, receiving block
3, display 4 and input device 5 are connected to proc-
essor 2. One example of a device as represented in
5 figure 1 could be a mobile station, which comprises
of a central processing unit along with the processors
1 and memories 2, the receiving block 3, display 4 and
the keyboard. Substantial in respect of the invention
in question is not the device itself by using which
10 the invention is realised, instead varied devices used
in electronic transactions may be possible.

In addition, the device as represented in
figure 1 comprises of means 12 for computing the check
sum at the program code, means 6 for adding the prede-
15 termined challenge to the program code and means 7 for
computing the aforementioned first check sum at the
combination of the program code and the challenge. In
one application, the means 7 and 12 may be imple-
mented, e.g. using a certified program code in which
20 case they are saved in the memory.

Moreover, the device as represented in figure
1 comprises of means 8 for storing the program and
challenge in the memory space and means 9 for computing
the check sum at the whole static memory space,
25 wherein the aforementioned program code and challenge
are stored. Moreover, the device comprises of equip-
ment 10 for receiving the challenge on the storage de-
vice via keyboard 5.

Fig. 2 represents the function of the inven-
30 tion in block diagram. The generator 26 of both the
challenge and the check sum is an outside certifica-
tion authority, another than the user 27, e.g. the
manufacturer of the program or a trusted third part,
which posses the original program code. The user re-
35 ceives the challenge and the corresponding check sum,
arrow 20, from an outside certification authority,
e.g. from its safe Internet sites. The user 27 acti-

vates the check prompt of the device, arrow 21. The device requests of the user for the challenge, which he/she inputs into the device, arrow 22. The device is, e.g. a mobile phone. The program code is read ac-
5 cording to the algorithm 28, arrows 23 and 24, and the check sum is computed using an appropriate method. The program code is located in the program memory 29. The check sum may be computed, e.g. using a hash function. Hash functions are, e.g. MD5 and SHA-1. The check sum
10 resulted from the application of algorithm 28 is re- turned to the user 27, who requested it, arrow 25. The user 27 reads the computed check sum, e.g. on the dis- play of his/her mobile phone and compares it with the check sum given by the outside certification author-
15 ity. If the check sums match, the program code of the device is valid.

    Substantial in the way of realising the checkout is the fact that the challenge is not known beforehand. For this reason, the check sum correspond-
20 ing to the challenge is impossible to anticipate. The challenge to be input has to be, in addition to that, long enough, in order to gain the wished reliability. Further, the check sum itself is not input into the program in which case the program cannot adapt itself
25 to the circumstances, in accordance with the check sum. When generating the check sum, the whole program code to be checked is read using an algorithm. The challenge and the program code are combined in such a way that the program cannot compute the combination of
30 the result of the checkout and the challenge corre- sponding to the original program code and consequently come to the right conclusion.

    Fig. 3 represents a preferred example of gen- erating the check sum as described in the invention.
35 The user wishes to make sure of the originality of the software he/she is using as described in the inven- tion. For the checkout, a random challenge 30 has been

generated using which the checkout is carried out. In this example the challenge 30 is a character string consisting of characters A, B, W, U, M and E. Each of the characters of the challenge 30 are located some-

5   where in the memory space 31. The location area is de-
fined by the location algorithm 32. The location algo-
rithm functions, e.g. in such a way that the character included in the challenge is added to a certain memory address of the memory area 31 or alternatively in such

10   a way that a certain computation operation is carried out between the character and the content of a certain memory address the outcome of which is located in the memory address in question. Arrow 33 shows the pro-
ceeding of the check algorithm. When all the charac-

15   ters included in the challenge have been located in the memory space 31 as wished, a check sum is computed at the whole memory area using, e.g. a hash algorithm. As an example of a hash algorithm let it be mentioned the MD5 and SHA-1 algorithms.

20   The invention may not be restricted to the examples of its applications described above, instead many variations are possible within the scope of the inventive idea defined in the claims.

CLAIMS

1. Method for authenticating a program code stored on a storage device, which method comprises of the following phases:
- a first check sum is computed at the program code,
- the check sum is compared with a second check sum known as valid and
- in response to the aforementioned comparison the program code is proved to be valid, in case the first check sum matches with the second check sum, c h a r a c t e r i s e d in that the method comprises of the following phases:
- a challenge is added to the program code, which challenge is chosen from a group including the character string, program function and input, in order to form the combination of the program code and challenge.
- the aforementioned first check sum is computed at the aforementioned combination.

2. Method as described in claim 1, c h a r - a c t e r i s e d in that the method comprises of the following phases:
- the said program code and the said challenge are stored in the memory space and
- the first check sum is computed at the whole memory space, wherein the aforementioned program code and challenge are stored.

3. Method as described in claim 1 or 2, c h a r a c t e r i s e d in that the said challenge and the check sum corresponding to it are chosen from a random group consisting of a set of challenges and check sums corresponding to them.

4. Method as defined in claim 1 or 2, c h a r a c t e r i s e d in that the length of the said challenge is chosen in such a way that the freed

memory cannot be used for storing the check sums cor-
responding to the challenges.

     5. Method as defined in claim 1, c h a r -
a c t e r i s e d in that an authenticated program code
is used for authenticating other program codes included
in the same software or system in such a way that the
check sum of an authenticated program code is compared
with the one given by other program codes over the same
challenge.

     6. Method as defined in claim 1, c h a r -
a c t e r i s e d in that the method, in addition,

     prevents the connection of the said storage
device with the outside world; and

     the validity of the program code is verified
in the storage device.

     7. Method as defined in claim 1, c h a r a c -
t e r i s e d in that the said challenge to be added to
the said program code is modified by using a certain
algorithm, in order to get a challenge of a standard
format.

     8. Device for authenticating the program
code, which device comprises of the following equip-
ment:

     - data-processing equipment (1),

     - storage device (2), which is connected with
the aforementioned data-processing equipment (1)

     - means (12) for computing the check sum at
the program code.

     - display (4), which is connected to the
aforementioned data-processing equipment and

     - keyboard (5), which is connected to the
aforementioned data-processing equipment, c h a r -
a c t e r i s e d in that the equipment comprises of:

     - means (6) for adding the predetermined
challenge, which is chosen from a group, which con-
sists of a character string, program function and in-
put, to the program code, as well as means for forming

14

the combination of the program code and the challenge
and

- means (7) for computing the first check sum
at the aforementioned combination.

5   9. Device as defined in claim 8, c h a r -
a c t e r i s e d in that the device comprises of:

- means (8) for storing the said program code
and said challenge in the static memory space and

- means (9) for computing the check sum at
10   the whole static memory space, wherein the said pro-
gram code and said challenge are stored.

10. Device as defined in claim 8 c h a r -
a c t e r i s e d in that the device comprises of means
(3) for receiving the said challenge at the storage
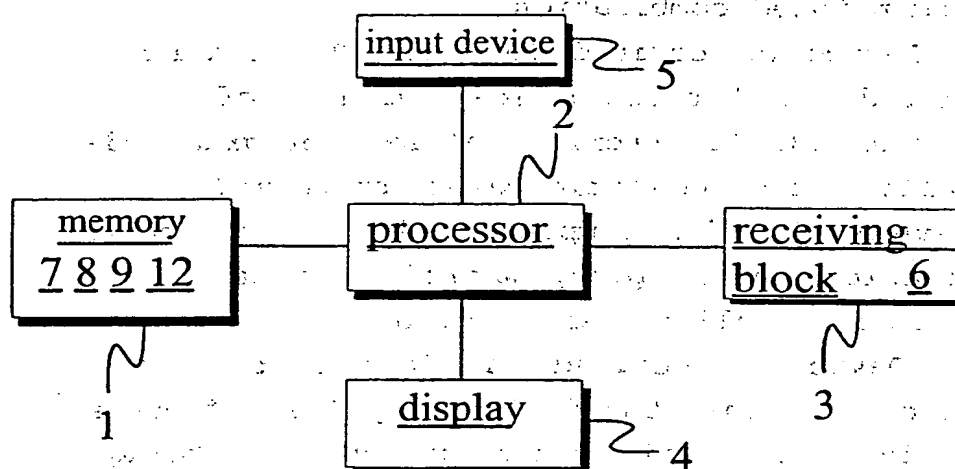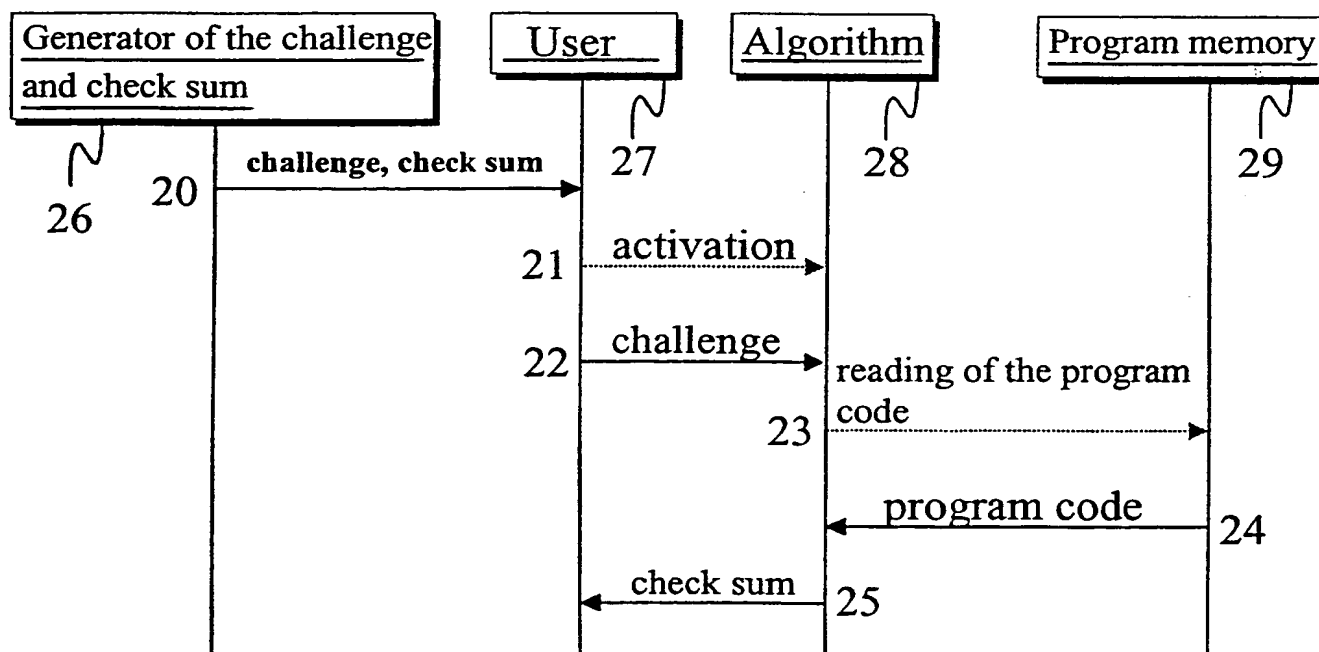15   device via keyboard (5).
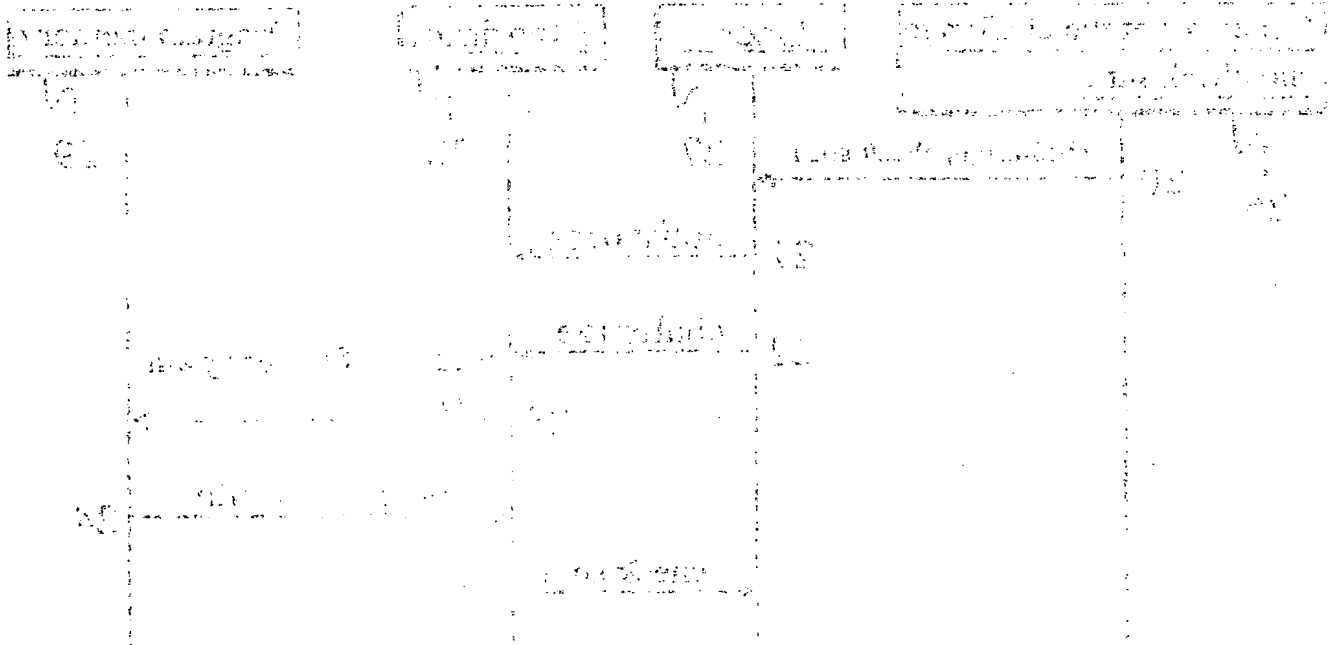
Fig. 1

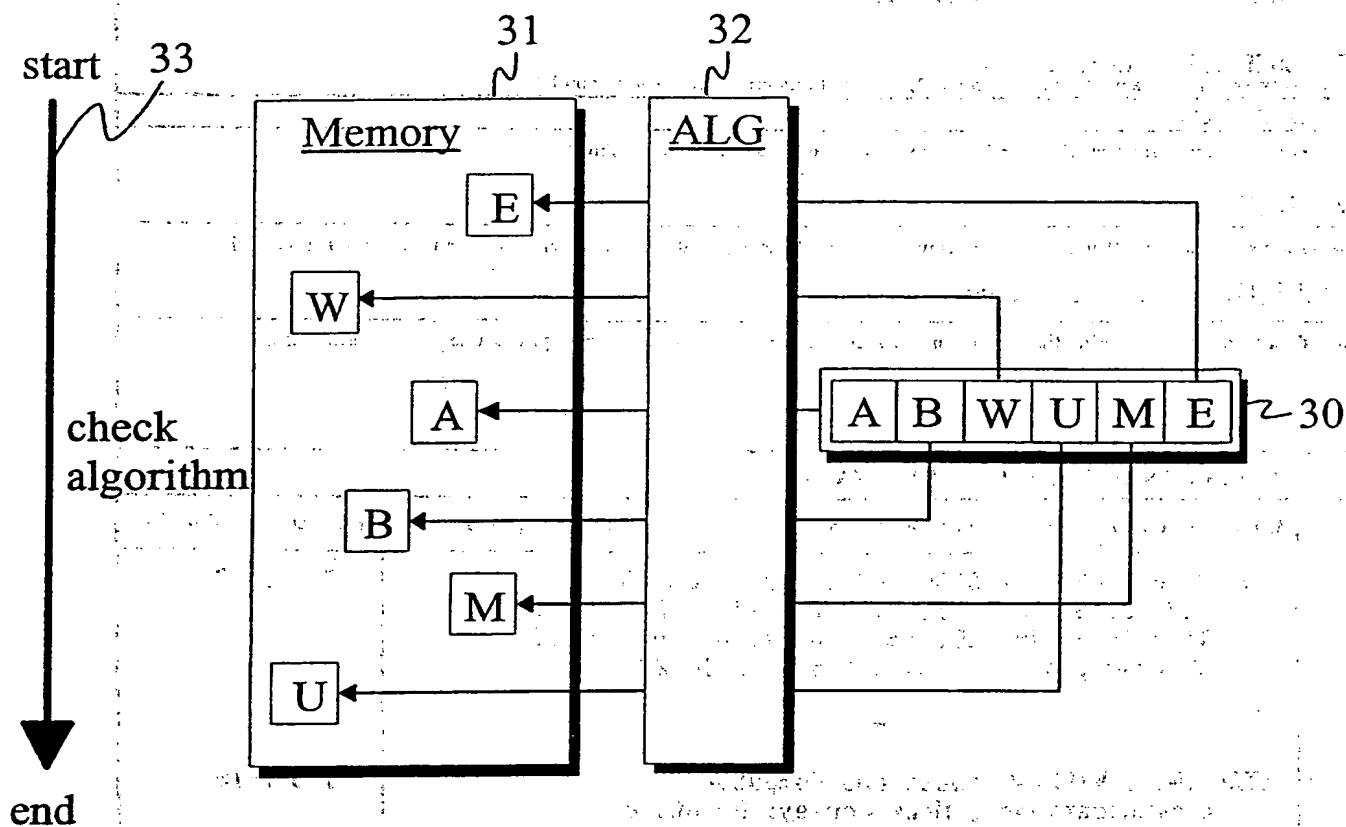Fig. 2

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00448

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 1/00, G06F 12/14
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9810611 A2 (ERICSSON INC.), 12 March 1998 (12.03.98), page 1, line 7 - line 12; page 9, line 16 - line 25; page 10, line 2 - line 12, abstract, see claims 1,2,5,8,11,14,27	1-5,7-10
X	STALLINGS, WILLIAM 'Data and Computer Communications', Neww Jersey: Prentice Hall Inc. 1997, ISBN 0-13-571274; pages 640-643, especially figure 18.11c	1-5,7-10
A	US 5224160 A (PAULINI ET AL), 29 June 1993 (29.06.93), claims 1,6,7	1-10

X	Further documents are listed in the continuation of Box C.		X	See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 August 2000	**2 4 -08- 2000**

Name and mailing address of the ISA	Authorized officer
Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Jan Silfverling/LR Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00448

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4593353 A (PICKHOLTZ), 3 June 1986 (03.06.86), See the whole document	1-10